Concluding Report for Phase 1[1]

Web-based Submission of the Discharge Monitoring Report[2]

EPA Contract #68-W5-0030[3]

Delivery Order #0004

Revised September 15, 1999

[1] Deliverable 7.2, InDyne, Inc., (formerly Information Dynamics, Inc.)

[2] A field test in the State of New York of the digital signing and submission of the Discharge Monitoring Report using an Adobe Acrobat Exchange plug-in to a Web browser as the electronic form environment which is connected interactively across the Internet to a receiving Web site. Cryptographic and handwritten biometric digital signatures are evaluated in this pilot.

[3] Submission of Environmental Data Under the Taiwan-USEPA Technical Cooperation Agreement

1 Scope

This document is a concluding report for Phase 1 of a pilot test of the Web-based submission of the New York State Discharge Monitoring Report (DMR) conducted in the State of New York June – November, 1999, beginning with the installation of the pilot hardware and software components on the pilot participant's computers in June of 1999 and ending with the conclusion of Phase 1 in August of 1999. The primary purpose of this report is to evaluate the results of Phase 1 in light of its objectives, where Phase 1 involves the application of hardware-based cryptographic signatures to a DMR form presented in an Adobe Acrobat Exchange electronic form environment which is in interactive communication over the Internet with a Web site.

The design of Phase 1, including the purpose of the pilot, motivation for the design of the pilot test environment and a description of the workflow involved in using the test environment is detailed in a separate Design Document. The purpose and functionality of hardware and software components used in Phase 1, and the specific commercial of-the shelf (COTS) products selected to fulfill these component functions, are discussed separately in a Requirements Document. The integration of COTS products to create the system used for the pilot test is described separately in "System Implementation". Technical issues identified in Phase 1 are discussed separately in the document, "Technical Issues in Phase 1". The number of DMRs received from each pilot participant, as well as detailed communications with the pilot participants, is given in the separate document, "Communications with Pilot Participants in Phase 1".

2 Overview of Phase 1 Results

Phase 1 of the pilot test of the electronic submission of the New York State Discharge monitoring report involved the use of an electronic form environment consisting of an Adobe Acrobat Exchange plug-in to a Netscape Navigator Web browser, where the electronic forms were digitally signed with a private key generated on a smart card. Phase 1 concluded with the pilot participants divided into two camps: those for whom the process worked and those for whom it didn't.

2.1 Successful Experience of the Pilot Participants

Of the seven pilot participants in Phase 1, four (General Electric, Montgomery County Sanitary District #1, Rosendale Waste Water Treatment Facility, and Indeck Energy Services) completed their Phase 1 assignment, which was to digitally sign and submit DMR form data associated with each discharge number in their permit for six historical reporting periods to the New York State Department of Environmental Conservation. In order to achieve their assignment, each of these pilot participants needed to:

- successfully install the DMR pilot's hardware and software components on their computer with an average install time of three hours,
- enroll their identity information with the certificate authority,
- use their smart card to generate a key pair and register their certificate with the certificate authority,
- log on to the pilot's Web site,
- select the appropriate monitoring period and discharge number using a menu structure,
- understand and use the Adobe electronic form environment to add data to the form,
- use their smart card and a digital signature plug-in to apply a digital signature to the form,
- submit the form data to the Web site,
- repeat the above three steps at least six times.

Typically the pilot participants who completed their assignment reported that the process of filling out the form was "easy enough after getting things set up" and "was the way to go" compared to the paper method. The fact that four out of seven pilot participants were successful in completing their Phase 1 assignment despite the lengthy setup procedure arguably demonstrates that it is possible to implement a method of signing and submitting an electronic DMR with a highly intuitive user interface for which the legal meaning of the digital signature is strong and the technical ability to authenticate the signature is high.

9.1 Challenges Encountered by the Pilot Participants

On the other hand, experience with Phase 1 of the pilot revealed that there are numerous difficult and maintenance-intensive technical issues involved in implementing an electronic reporting configuration that requires:

- the installation of external hardware on the serial port of the computer,
- the integrated use of sophisticated cryptographic software and hardware components supplied by the smart card manufacturer, the operating system and the digital signature software provider,
- a high level of compatibility among the Web browser, the electronic form plug-in, the digital signature plug-in, the smart card software, the operating system, the external Web site and the certificate authority server,
- the maintenance of multi-vendor compatibility through changes in versions of each software component,
- the availability of a reliable network connection over wide geographical distances and across different firewall configurations.

The experience of the three pilot participants (IBM, Allied Signal and the Village of Champlain) who were not successful in completing their Phase 1 assignment illustrates that the impact of even a minor problem in a complex system can be a powerful technical and psychological roadblock to a successful result. IBM first experienced a problem in registering their certificate because of their firewall and then disabled their smart card by typing an incorrect PIN code more than three times. Allied Signal experienced just enough small technical issues with their NT computer and their firewall that the priorities of the pilot didn’t survive the triage of other pressing demands.

The Village of Champlain experienced more difficult technical problems in the installation of the smart card and the functioning of the cryptographic components on their computer, to the extent that diagnostic tests would need to have been run to do effective troubleshooting. Although the computer used by the Village of Champlain may have been more complex than most (e.g., a digital camera was installed on the serial port needed for the smart card) the technical problems encountered may have been the “hand that was dealt” in the sense that the experience of the Village of Champlain revealed what can go wrong in a system of many variables.

14.1 Possible Interpretations of Phase 1 Results

In the broad view, therefore, the results of Phase 1 tell a “good news – bad news” story:

♦ **The good news:**

- The Adobe Acrobat Exchange form provided an intuitive and easily understood electronic form environment for the DMR.
- A digital signature plug-in to the Adobe Acrobat Exchange form could sign the entire contents of the form as it was represented electronically in the signer’s computer at the moment of signing.
- The public key infrastructure established for the pilot allowed the certificate authority and local registration authority roles to be implemented in a meaningful and effective way.
- When everything worked as intended, the process of filling out and signing the electronic DMR was quick and effective.

♦ **The bad news:**

- In an environment in which the computing environment used by the submitter’s cannot be strictly controlled, the number of variables involved in setting up an interactive electronic form environment with hardware-based cryptographic digital signatures is large and contributes to the need for substantial technical support and maintenance.
- When technical problems occur, it may cause a potential user of the electronic reporting system to become discouraged and fail to take the steps needed to achieve a working solution.
- The higher the need for the legal validity of the signature and the technical ability to authenticate the signature, the higher the complexity of the electronic reporting solution.

8.0.1 The Role of a Legal Value Question in Interpreting Pilot Results

An interpretation of the results of Phase 1 depend on the degree of importance, emphasis and value placed on the following legal consideration:

- “Can a reasonable person be persuaded that a particular individual signed a given electronic form, and understood the meaning of this signature?”

The pilot test environment was designed based on the assumption that the value of the above question is high. As a result, the pilot environment contains many elements (e.g., smart cards, Adobe forms, etc.) which arguably contribute to a meaningful context for a digital signature and a relatively high technical confidence that the signer can be linked to the contents of the submitted form. The results from Phase 1 of the DMR pilot show that such an environment can be technically achieved, but at a high installation, setup, maintenance and technical support cost.

If the value of legal considerations related to signature issues is considered high, then one interpretation of the Phase 1 pilot result could be that one should implement as many components as possible which support meaningful digital signatures, but delay the introduction of components such as smart cards (for example) until such time as smart cards are widely used by the general public and computers are made with built-in smart card readers. Another interpretation consistent with a high value placed on signatures and authentication would be to incrementally improve the stability of the submission system through the natural and anticipated upgrading and maturing of its components. During in-house testing, for example, there was evidence that a system built on GemSAFE 2.0, Adobe Acrobat Exchange 4.0, HAHTsite 4.0, etc., would work more smoothly than the pilot environment, which was based on GemSAFE 1.0, Adobe Acrobat Exchange 3.01, HAHTsite 3.1, etc. Alternatively, time may prove the emergence of a historical track record for the ability of XML-enabled Web browsers, for example, to consistently render a standardized electronic representation of content.

If, on the other hand, the value of the signature/authentication issue is not seen as that important compared with the practical need to collect compliance data from as many people, companies and organizations as possible within the shortest implementation time, then the Phase 1 pilot test results caution against the complexity introduced by:

- introducing any new hardware or software component to the submitter’s computer,
- adding additional procedural steps,
- relying upon compatibility and interfaces among many different software components from different manufacturers.

Solutions which do not install anything new on the submitter’s computer must be limited in functionality to what can be supported by a broad cross-section of Web browsers, for example. However the ActiveX and Java technology currently available to make the electronic form environment sufficiently functional for multi-page and multi-line forms also adds complexity to the solution, and is not permitted due to security concerns in some companies and organizations.

13 Pilot Results Compared with Evaluation Factors

This section will compare the Phase 1 pilot results with evaluation factors established as questions in the Design Document related to Phase 1.

13.1 Questions Related to Digital Signatures

Pilot results related to digital signature questions are discussed following each question below:

- ♦ Can a workable public key infrastructure be established which links the signer’s private cryptographic key to the signer’s identity by means of a security policy which can be used by the New York State Department of Environmental Conservation (NYS DEC) and the pilot participants and which also binds the private key to the signer’s identity with a sufficient level of assurance?

Although three pilot participants (Allied Signal, IBM and the Village of Champlain) experienced difficulty in some aspect of the certificate registration process, the pilot results demonstrated that a workable public key infrastructure could be established for the pilot. NYS DEC successfully used the local registration authority administrative console provided by the certificate authority to approve enrollments and manage certificates issued to the pilot participants. Pilot participants who were not blocked by a firewall or a problem with the cryptographic services on their local computer (as was experienced by the Village of Champlain) were able to complete the process of enrolling with the certificate authority, receiving a one-time access code by E-mail from the certificate authority based on the approval of their identity information by the local registration authority, and then registering their certificates with the certificate authority across the Internet. An alternative means of completing the certificate registration process using a Web browser was developed during Phase 1 to allow those pilot participants behind firewalls to complete the registration process. This method was successful for one pilot participant, General Electric, and may have worked also for Allied Signal and IBM if it were tried.

- ♦ Can private keys be implemented on a hardware token (smart card) in a manner which is usable by the pilot participants and is compatible with a mechanism for applying cryptographic signatures to the DMR?

The pilot results demonstrated that a smart card could be successfully used to apply digital signatures to electronic DMR forms. However, the Phase 1 experience revealed that the smart cards introduced a higher level of complication (compared with software-based cryptographic key generation) due to competition for what for most pilot participants was a single available serial port, conflicts with other software installed to use the serial port, unexpected side effects (e.g., blue screens on shut down, disabling energy saving features, affecting the graphics accelerator card settings, etc.) and user issues (e.g., forgetting PIN numbers, needing to know when to insert the smart card into the reader).

15.1 Questions Related to Human Factors

Pilot results related to human factors are discussed following each question below:

- How long and how difficult will the pilot participants find the process of installing the hardware and software components needed for the pilot? What average times and kinds of difficulty are experienced in each installation step?

Actual experience of the pilot participants with the hardware and software installations showed that the average install time was three hours, beginning with the installation or upgrade of the Web browsers needed for the pilot. Two pilot participants experienced problems reading some of the install CDs. Several pilot participants experienced difficulty following the manufacturer's directions for installing the smart card reader hardware. Although most of the pilot participants could perform most of the install steps based on an installation guide prepared for the pilot, no pilot participant completed all steps without some advice or help from the NYS DEC or InDyne staff.

- Will the pilot participants understand the meaning and purpose of digital signatures? Will the concept of digital signatures be accepted as intuitively obvious? What types of errors related to the submitter's understanding of the digital signature will emerge? What types of technical errors will emerge?

Although the pilot participants intuitively understood that clicking the signature icon located on the last page of the electronic form constituted their signing of the form, some pilot participants invalidated the cryptographic digital signature by making changes to the form after it had been signed. This demonstrated that the pilot participants did not understand the way a cryptographic digital signature operates. In one case (the Village of Champlain), the digital signature failed for technical reasons, probably due to an unstable or corrupted cryptographic service on the signer's computer which would have required either resetting the service by reinstalling a new certificate or reinstalling the cryptographic service component.

- How will the pilot participants experience the setup processes required to participate in a public key infrastructure for the purpose of using a cryptographic digital signature?

All pilot participants experienced the enrollment of identity information with the Web browser to be easy and straightforward, with the exception of General Electric, where the fields in the enrollment form did not display until the pilot participant clicked on them. This behavior was probably due to either a setting in the participant’s Web browser that determines how frequently Web pages are refreshed, or possibly a graphics accelerator setting.

Three pilot participants (General Electric, Allied Signal, and IBM) experienced difficulty in completing the registration process due to the presence of a firewall, and one participant (the Village of Champlain) experienced a problem when attempting to re-register a certificate, probably because the local cryptographic service was corrupted and needed to be reinstalled.

- ♦ How intuitive will the pilot participants find the electronic forms environment used to display the contents of the DMR form and accept data entry from the submitter?

The pilot participants immediately understood the presentation of the DMR within the Adobe Acrobat Exchange electronic form environment. This was evidenced by the lack of questions on this subject and the speed at which the pilot participants began entering data into the form.

- ♦ How intuitive will the pilot participants find the process of using the receiving Web site, including the process of logging into the receiving Web site, finding and selecting the appropriate DMR?

The pilot participants seemed to understand the concept of logging in to the Web site and navigating its menu selections. One pilot participant (Rosendale WWTF) stated that the provision for multiple versions of DMR forms was confusing.

20.1 Questions Related to Implementation Options

Pilot results related to implementation of the DMR pilot are discussed following each question below:

- ♦ What compatibility restrictions will be discovered among the different software products used to produce the integrated functionality for the pilot?

The differences in the behavior of the integrated system when different manufacturers or versions of products were used were more extreme than anticipated. HAHTsite application server Version 3.1 triggers the opening of multiple windows of Adobe Acrobat Exchange 3.01 forms when the browser is Internet Explorer 4.01, but not when the browser is Netscape Navigator 4.51. Multiple Adobe windows do not open within Internet Explorer 4.01 if Adobe Acrobat Exchange Version 4.0 is used instead of Version 3.01. The use of Netscape Navigator 4.51 with Secure Sockets Layer (SSL) reduces the number of Adobe Acrobat Exchange 3.01 form pages which can receive data from the HAHTsite application server Version 3.1, but this behavior does not occur with Internet Explorer 4.01.

- What specific problems or behaviors will be observed when the pilot participants install hardware devices on their computers?

The installation of the smart card reader produced dramatic side effects on some pilot participant's computers, such as a blue screen error when shutting down the computer. The solution to this problem, an update of the Microsoft smart card driver library, was equally surprising. One pilot participant (the Village of Champlain) reported screen lockups after installing the smart card. He resolved this problem by reducing his graphics accelerator setting and screen scrolling speed. The introduction of a hardware device on the only available serial port of the pilot participant's computer sometimes revealed software conflicts for the use of the serial port with symptoms which were initially hard to diagnose. For example, IBM noticed that access to the Internet became slower and less reliable after the smart card was installed. This was ultimately traced to a conflict for the serial port interrupt between an internal modem and the smart card, even though the modem was not directly attached to the serial port.

- Will the configuration of software and hardware components installed for the DMR pilot behave similarly across all of the pilot participants' computers, or will differences in some or all pilot participants' computers result in a divergent set of behaviors observed for the installed hardware/software configuration?

An unexpectedly diverse distribution of behaviors was seen when the same hardware and software components were installed on the different pilot participant's computers, as was illustrated by the diversity of technical issues encountered across multiple pilot participant sites.

- Will the pilot participants experience difficulty in connecting to the receiving Web site established for the DMR pilot across their respective network connections, including dial-up lines?

In general, pilot participants were able to access, log on, and use the receiving Web site across firewalls and over a variety of different network connections. General Electric reported at one point that the application server at the receiving Web site was denying access. This was believed to be due to a mechanism employed at General Electric to balance the network traffic load between two or more firewalls. The application server detected that the General Electric computer seemed to be switching Internet Protocol (IP) addresses and blocked access for security reasons. This security feature was disabled to allow General Electric to use the Web site.

- Will the pilot participants or the Local Registration Authority administrator experience difficulty in connecting to the certificate authority server across their respective network connections?

In general the Local Registration Authority administrator was able to connect to the certificate authority server whenever necessary. Pilot participants located behind firewalls could not initially access the certificate authority server for the purpose of registering certificates. The Village of Champlain could not access the certificate authority server to re-register a new certificate.

- ♦ Can the pilot participants switch between standard Web pages and the electronic form environment with acceptable responsiveness?

The electronic form sometimes required as much as 20 seconds to load pre-populated data from the receiving Web site. Other than this delay, the transition between standard HTML Web pages and the Adobe Acrobat Exchange electronic form pages was a workable environment for the pilot participants.

- ♦ Will the process of pre-populating the DMR forms with data from the receiving site’s database occur with reasonable responsiveness?

In most cases, the DMR forms receive their pre-populated data from the Web site within a few seconds. In some cases, particularly with longer forms, this loading process was observed to take up to 20 seconds.

- ♦ Can the digital signature applied to the DMR form by the submitter be verified at the receiving site with sufficient speed to notify the submitter of the success or failure to verify shortly after the DMR form is submitted to the receiving site?

Yes, the digital signature was verified at the receiving Web site almost immediately after the submit button was pressed by the pilot participant.

- ♦ Can the New York State Department of Environmental Conservation successfully receive the submitted data files shortly after the submitted DMR data have been received?

Submitted data files were automatically packaged as structured files within attachments to E-mail messages which were mailed to the New York State Department of Environmental Conservation within an hour after the data were received from the submitter.

- ♦ Is the version control applied to the submitted components of the DMR (e.g., discharge numbers and comments) sufficient for the New York State Department of Environmental Conservation to determine which components should be assembled to form a completed DMR and also to distinguish the most recent submission of any component from previous submitted versions?

Yes, the convention of internal and external version numbers applied to the DMR form components proved to be a workable method of tracking versions.

- ♦ What scalability, maintainability, compatibility or security issues are raised by the specific implementation used for the DMR pilot?

The need for a high level of personalized technical support in installation and troubleshooting prevents the current submission system from being scaled to large numbers of participants. It is possible that the individual products supplying the Web browser, electronic form, digital signature and smart card functions would become more stable as they mature. The greatest difficulties are experienced in setting up the environment. Once the submission system was established successfully for a given participant, it continued to operate in a stable manner.

- What alternative implementation options are suggested by the pilot experience?

Performing cryptographic functions in software rather than using a smart card would remove a significant element of complexity from the submission system. Testing upgraded versions of the component products would probably result in fewer technical problems.

If the particular user interface and legal considerations favoring the Adobe Acrobat Exchange electronic form product were not considered as important, a logical alternative architecture would be to attempt to create a workable electronic form environment without requiring the installation of additional software on the submitter's computer. ActiveX and Java could be used for this purpose, but the fact that each form would be the product of customized programming would reduce the credibility of the resulting electronic form as having well-known and trusted properties which had been proven over time. Such an approach would also be a security concern for some companies and organizations.

33 Summary of Conclusions

The following subsections discuss an overview of the principal conclusions suggested by Phase 1 of the DMR pilot.

33.1 Conclusions Related to Receiving Signed DMR Data

Phase 1 of the DMR pilot in the State of New York demonstrated that the Adobe Acrobat Exchange electronic form environment was received by the pilot participants as an intuitive and easily understood method to submit DMR data over the Internet to a receiving Web server. Signed DMR data received at the Web server could be authenticated and transmitted to the New York State Department of Environmental Conservation (NYS DEC) reliably. The method of applying cryptographic digital signatures to the electronic DMR form successfully achieved the following desired results:

- The submitter's identity was strongly bound to a smart-card generated private cryptographic key used as input to the signature algorithm by means of a complete public key infrastructure in which NYS DEC acted as the local registration authority.
- The electronic representation of the complete contents of the DMR form (template plus data) was signed in context at the time the submitter executed the signature using an electronic form environment in which the consistent correspondence between the electronic representation of the DMR form and its visible representation to the signer can be argued by de facto historical experience with the commercial off-the-shelf electronic form product (Adobe Acrobat Exchange).
- The receiving Web server was able to automatically verify the signature and apply a timestamp to the DMR data received from the submitter across the Internet.

NYS DEC was able to verify that the DMR data they received from the electronic submissions was consistent with historical paper DMR submissions with the exception of some formatting differences, since the paper DMR submissions did not enforce as rigorous format requirements for some data fields as did the electronic form.

36.1 Conclusions Related to Client-side Hardware & Software

The same hardware and software elements which were designed to achieve the above desired signature results (an electronic form with consistent content representation signed by a hardware-based digital signature supported by a public key infrastructure with an on-line Internet submission process) also created the need for a lengthy install process on the submitter's computers and generated a broad range of technical difficulties experienced to a greater or lesser degree by each of the pilot participants. The more significant of these technical issues can be summarized in the following broad categories:

- The installation of the smart card reader created side-effects on some of the pilot participant's computers with different manifestations on different computers, including serial port conflicts, errors on shut-down, failure to return to power-saving mode, or screen lock-ups.
- The use of the smart card added complexity to the install and signing process if the pilot participant failed to remember the 4-digit personal identification number needed to activate the card, or if the pilot participant inserted the smart card into the smart card reader after the Web browser had already launched.
- The process of registering the X.509 certificate containing the participant's identity information and public key proved difficult for some participants

due to the presence of a firewall or to the health of the cryptographic services installed on their computer.

- The Adobe Acrobat Exchange Version 3.01 electronic form did not exhibit identical behavior on all pilot participants' computers with respect to the loading of pre-populated default data across the Internet from the Web server. In some cases the loading of data did not succeed the first time, or was slower than expected. In other cases, the presence of the digital signature plug-in changed the visibility of the cursor or the color of some of the form fields depending upon the screen resolution and color density setting on the pilot participant's computer.

In the DMR pilot, the pilot participants used a uniform configuration of added software and hardware components needed for the pilot, which were installed in addition to the pilot participant's own previous hardware and software configuration on computers provided by the pilot participants. This uniform configuration included a specified manufacturer and version of a Web browser for particular DMR pilot functions. Testing prior to the installation of hardware and software components on the pilot participants' computers revealed additional technical issues related to the compatibility of some of the software components with each other. The more significant of these issues included:

- The behavior of the Adobe Acrobat Exchange Version 3.01 form plug-in in a Secure Sockets Layer connection with the Web server was dependent upon the Web browser used. Netscape Navigator Version 4.51 allowed data for fewer form pages to be downloaded from the application server at the Web site than did Microsoft Internet Explorer Version 4.01, presumably because of a higher memory overhead needed by Netscape Navigator when SSL was used.

- The behavior of the Web browser when launching Adobe Acrobat Exchange Version 3.01 in response to receiving a form template from the Web server was dependent upon the Web browser used. Adobe Acrobat Exchange launched in separate windows when Microsoft Internet Explorer Version 4.01 was used, and in one window when Netscape Navigator Version 4.51 was used.

These in-house test results demonstrate that a combination of an electronic form and a Web browser will produce different behaviors depending on the manufacturer and version of both the electronic form and the browser. Therefore, in a production environment, supported combinations of electronic form and Web browser products and versions would need to be specified and tested.

The variety of behaviors and technical issues encountered when installing and running the pilot hardware and software components on the pilot participants' computers suggest that the task of defining, installing, maintaining and supporting configurations of these components in a wider production environment would be challenging and costly, and that the technical problems encountered may not be uniformly tolerated by the submitters if the purpose of these components were limited to the submission of DMRs. This assessment is tempered by the following considerations:

- With time, the electronic form, signature and browser components would be reasonably expected to mature and be more widely used.
- The functionality supplied by one or more of these components may prove essential to the legal requirement to link the signer's identity to the content of the form in a paperless environment.

44.1 Conclusions Related to Possible Design Options

The DMR submission environment could be simplified by dropping one or more of the hardware or software components from the submission process, with a corresponding reduction in some functionality or the possible introduction of alternative problems. The following table identifies some of these options and consequences. The table should be read as follows, "For each row of the table, if the functionality listed in the first column is removed (assuming all other components of the original DMR pilot hardware/software configuration are retained), then the consequences listed in the second column would be expected as a result."

Functionality Removed	Consequence
Removal of Adobe Exchange electronic form	1) Reduces the ability to assert that the visual representation of the form corresponds to the digitally-signed electronic representation. 2) Reduces the ability to present a consistent user interface that displays the form with a familiar visual representation and to provide an intuitive and well-known set of electronic form tools. 3) Form functionality would need to be replaced with Java, ActiveX or some other customized mechanism that has less of a demonstrable history of consistent and accurate visual content representation across all browsers and platforms.
Removal of integration of Adobe	1) Eliminates the ability to receive

Exchange form with a Web browser	prepopulated default form data and send submitted data using normal Web HTTP transport mechanisms. 2) Weakens the chain of custody between the submitter and the receiving site.
Removal of hard-ware based generation of private cryptographic keys by smart cards	Reduces the protection of the private key, with the possible long-term reduction in the ability to assert the binding of the private key to an individual.
Removal of a digital signature executed by the submitter	Reduces the ability to demonstrate that the submitter assented to the specific contents of the submitted DMR.

As the above table illustrates, the submission environment can be simplified at the expense of removing functionality that may be judged to serve a necessary purpose. Any possible alternate design options for a submission environment for the DMR will be caught somewhere in this tension. The experience of Phase 1 suggests that a submission environment designed to achieve a relatively high level of signature authentication and security can be achieved, but the setup of such an environment will be initially time consuming for the submitter and may involve a variety of technical problems which are dependent upon the submitter's computing environment or particular DMR form or data. Therefore the support costs of such an environment would be predictably high. Phase 1 results seem to indicate, however, that once installation and initial technical problems are resolved, that the submission environment can be subsequently maintained in a manner which the submitters describe as easy to use.